WHAT IS CLAIMED IS:

sub A1

1. A method for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device, said method comprising:

partitioning at least a portion of said storage device to form a security partition having at least one authority record and at least one data set associated with said authority record;

limiting access to at least a portion of said storage device by said operating system of said computer system.

2. The method of Claim 1, wherein said computer system includes a networked computer system.

3. The method of Claim 1, wherein at least a portion of said storage device firmware comprises writeable firmware.

4. The method of Claim 1, wherein at least a portion of said storage device firmware comprises non-writeable firmware.

5. The method of Claim 1, further comprising transporting data to said storage device only in connection with execution of said firmware of said storage device.

6. The method of Claim 1, wherein said storage device is configured in accordance with a protocol selected from the group consisting of ATA protocol and SCSI protocol.

7. The method of Claim 1, wherein said partitioning step occurs on a low-level formatting portion of said storage device.

8. The method of Claim 1, further comprising adding data to said storage device in an orientation selected for promoting identification of remaining data storage space on said storage device.

9. The method of Claim 1, further comprising said security partition having a master authority record.

10. The method of Claim 9, further comprising said master authority record governing all said authority records in said storage device.

11. The method of Claim 1, further comprising translating information from a master authority record included in said storage device to a group authority in said operating system.

12. The method of Claim 1, further comprising writing said security partition using a security partition open call.

13. The method of Claim 12, further comprising closing said security partition after a predetermined time interval.

14. The method of Claim 1, further comprising reading said security partition using a security partition open call.

15. The method of Claim 14, further comprising closing said security partition after a predetermined time interval.

16. The method of Claim 1, wherein said authority record includes a public-private key pair for authenticating data originating from said security partition.

17. The method of Claim 16, wherein said authority record includes a second public-private key pair for ensuring data can only be sent to said security partition and no other location for storing said data.

18. The method of Claim 1, further comprising storing a symmetric key on said storage device.

19. The method of Claim 1, further comprising using a private key for decoding a passcode transmitted to said authority record of said storage device.

20. The method of Claim 1, further comprising encrypting at least a portion of said data in said security partition.

21. The method of Claim 1, further comprising encrypting data on said storage device so that only an external agent can decrypt said encrypted data.

22. The method of Claim 1, further comprising providing no method for decrypting data stored on said storage device with information available on said storage device.

23. The method of Claim 1, further comprising hiding at least one field of said authority record.

24. The method of Claim 1, further comprising storing a hash of code in a passcode field of said authority record.

25. The method of Claim 1, further comprising securing a symmetric key by encrypting said symmetric key with a public key of said authority record, and hiding a private key in said authority record, thereby permitting only said hidden private key to decode said symmetric key.

26. The method of Claim 1, further comprising storing at least one public key in said storage device.

27. The method of Claim 1, further comprising storing at least one private key in said storage device.

28. The method of Claim 1, further comprising declaring at least a portion of data in said security partition to be write-once.

29. The method of Claim 1, further comprising permitting only a predetermined user to access a master authority record of said security partition.

30. The method of Claim 1, wherein said authority record includes at least one nonce.

31. The method of Claim 30, further comprising encrypting said nonce with a public key.

32. The method of Claim 1, wherein said authority record includes at least one time value associated with processing of a portion of data stored on said storage device.

33. The method of Claim 32, wherein said time value is selected from the group consisting of a start time and an end time.

34. The method of Claim 1, further comprising storing call authentication data on said storage device.

35. A system for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device, said system for promoting security comprising:

a security partition formed in said storage device having at least one authority record and at least one data set associated with said authority record;

wherein access to said security partition in said storage device by said operating system of said computer system is limited.

36. The system of Claim 35, wherein said computer system includes a networked computer system.

37. The system of Claim 35, wherein at least a portion of said storage device firmware comprises writeable firmware.

38. The system of Claim 35, wherein at least a portion of said storage device firmware comprises non-writeable firmware.

39. The system of Claim 35, wherein said storage device is configured in accordance with a protocol selected from the group consisting of ATA protocol and SCSI protocol.

40. The system of Claim 35, wherein said security partition is formed on a low-level formatting portion of said storage device.

41. The system of Claim 35, further comprising said security partition having a master authority record.

42. The system of Claim 41, further comprising said master authority record being in operative association with a group authority in said operating system.

43. The system of Claim 35, wherein said authority record includes a public-private key pair for authenticating data originating from said security partition.

44. The system of Claim 43, wherein said authority record includes a second public-private key pair for ensuring data can only be sent to said security partition and no other location for storing said data.

45. The system of Claim 35, further comprising a symmetric key stored on said storage device.

46. The system of Claim 35, further comprising encrypted data stored on said storage device.

47. The system of Claim 35, further comprising at least one hidden field in said authority record.

48. The system of Claim 35, further comprising said authority record having a passcode field.

49. The system of Claim 35, further comprising a hidden key stored in said storage device.

50. The system of Claim 35, further comprising at least one public key stored in said storage device.

51. The system of Claim 35, further comprising at least one private key stored in said storage device.

52. The system of Claim 35, wherein said authority record includes at least one nonce.

53. The system of Claim 35, wherein said authority record includes at least one time value associated with processing of a portion of data stored on said storage device.

54. The system of Claim 53, wherein said time value is selected from the group consisting of a start time and an end time.

55. The system of Claim 35, further comprising call authentication data stored on said storage device.

56. A computer-readable medium containing instructions for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device, said medium comprising:

instructions for partitioning at least a portion of said storage device to form a security partition having at least one authority record and at least one data set associated with said authority record;

instructions for limiting access to at least a portion of said storage device by said operating system of said computer system.

57. The medium of Claim 56, wherein said computer system includes a networked computer system.

58. The medium of Claim 56, wherein at least a portion of said storage device firmware comprises writeable firmware.

59. The medium of Claim 56, wherein at least a portion of said storage device firmware comprises non-writeable firmware.

60. The medium of Claim 56, further comprising instructions for transporting data to said storage device only in connection with execution of said firmware of said storage device.

61. The medium of Claim 56, wherein said storage device is configured in accordance with a protocol selected from the group consisting of ATA protocol and SCSI protocol.

62. The medium of Claim 56, wherein said instructions for partitioning include instructions for partitioning in a low-level formatting portion of said storage device.

63. The medium of Claim 56, further comprising instructions for adding data to said storage device in an orientation selected for promoting identification of remaining data storage space on said storage device.

64. The medium of Claim 56, further comprising said security partition having a master authority record.

65. The medium of Claim 64, further comprising said master authority record including instructions for governing all said authority records in said storage device.

66. The medium of Claim 56, further comprising instructions for translating information from a master authority record included in said storage device to a group authority in said operating system.

67. The medium of Claim 56, further comprising instructions for writing said security partition using a security partition open call.

68. The medium of Claim 67, further comprising instructions for closing said security partition after a predetermined time interval.

69. The medium of Claim 56, further comprising instructions for reading said security partition using a security partition open call.

70. The medium of Claim 69, further comprising instructions for closing said security partition after a predetermined time interval.

71. The medium of Claim 56, wherein said authority record includes a public-private key pair for authenticating data originating from said security partition.

72. The medium of Claim 71, wherein said authority record includes a second public-private key pair for ensuring data can only be sent to said security partition and no other location for storing said data.

73. The medium of Claim 56, further comprising instructions for storing a symmetric key on said storage device.

74. The medium of Claim 56, further comprising instructions for using a private key for decoding a passcode transmitted to said authority record of said storage device.

75. The medium of Claim 56, further comprising instructions for encrypting at least a portion of said data in said security partition.

76. The medium of Claim 56, further comprising instructions for encrypting data on said storage device so that only an external agent can decrypt said encrypted data.

77. The medium of Claim 56, further comprising instructions for hiding at least one field of said authority record.

78. The medium of Claim 56, further comprising instructions for storing a hash of code in a passcode field of said authority record.

79. The medium of Claim 56, further comprising instructions for securing a symmetric key by encrypting said symmetric key with a public key of said authority record, and instructions for hiding a private key in said authority record, thereby permitting only said hidden private key to decode said symmetric key.

80. The medium of Claim 56, further comprising instructions for storing at least one public key in said storage device.

81. The medium of Claim 56, further comprising instructions for storing at least one private key in said storage device.

82. The medium of Claim 56, further comprising instructions for declaring at least a portion of data in said security partition to be write-once.

83. The medium of Claim 56, further comprising instructions for permitting only a predetermined user to access a master authority record of said security partition.

84. The medium of Claim 56, wherein said authority record includes at least one nonce.

85. The medium of Claim 84, further comprising instructions for encrypting said nonce with a public key.

86. The medium of Claim 56, wherein said authority record includes at least one time value associated with processing of a portion of data stored on said storage device.

87. The medium of Claim 86, wherein said time value is selected from the group consisting of a start time and an end time.

88. The medium of Claim 56, further comprising instructions for storing call authentication data on said storage device.

89. A system for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device, said system for promoting security comprising:

means for partitioning at least a portion of said storage device to form a security partition having at least one authority record and at least one data set associated with said authority record;

means for limiting access to at least a portion of said storage device by said operating system of said computer system.

90. The system of Claim 89, wherein said computer system includes a networked computer system.

91. The system of Claim 89, wherein at least a portion of said storage device firmware comprises writeable firmware.

92. The system of Claim 89, wherein at least a portion of said storage device firmware comprises non-writeable firmware.

93. The system of Claim 89, further comprising means for transporting data to said storage device only in connection with execution of said firmware of said storage device.

94. The system of Claim 89, wherein said storage device is configured in accordance with a protocol selected from the group consisting of ATA protocol and SCSI protocol.

95. The system of Claim 89, wherein said means for partitioning partitions a low-level formatting portion of said storage device.

96. The system of Claim 89, further comprising means for adding data to said storage device in an orientation selected for promoting identification of remaining data storage space on said storage device.

97. The system of Claim 89, further comprising said security partition having a master authority record.

98. The system of Claim 97, further comprising means for said master authority record to govern all said authority records in said storage device.

99. The system of Claim 89, further comprising means for translating information from a master authority record included in said storage device to a group authority in said operating system.

100. The system of Claim 89, further comprising means for writing said security partition using a security partition open call.

101. The system of Claim 100, further comprising means for closing said security partition after a predetermined time interval.

102. The system of Claim 89, further comprising means for reading said security partition using a security partition open call.

103. The system of Claim 102, further comprising means for closing said security partition after a predetermined time interval.

104. The system of Claim 89, wherein said authority record includes a public-private key pair for authenticating data originating from said security partition.

105. The system of Claim 104, wherein said authority record includes a second public-private key pair for ensuring data can only be sent to said security partition and no other location for storing said data.

106. The system of Claim 89, further comprising means for storing a symmetric key on said storage device.

107. The system of Claim 89, further comprising means for using a private key for decoding a passcode transmitted to said authority record of said storage device.

108. The system of Claim 89, further comprising means for encrypting at least a portion of said data in said security partition.

109. The system of Claim 89, further comprising means for encrypting data on said storage device so that only an external agent can decrypt said encrypted data.

110. The system of Claim 89, further comprising means for providing no system for decrypting data stored on said storage device with information available on said storage device.

111. The system of Claim 89, further comprising means for hiding at least one field of said authority record.

112. The system of Claim 89, further comprising means for storing a hash of code in a passcode field of said authority record.

113. The system of Claim 89, further comprising means for securing a symmetric key by encrypting said symmetric key with a public key of said authority record, and means for hiding a private key in said authority record, thereby permitting only said hidden private key to decode said symmetric key.

114. The system of Claim 89, further comprising means for storing at least one public key in said storage device.

115. The system of Claim 89, further comprising means for storing at least one private key in said storage device.

116. The system of Claim 89, further comprising means for declaring at least a portion of data in said security partition to be write-once.

117. The system of Claim 89, further comprising means for permitting only a predetermined user to access a master authority record of said security partition.

118. The system of Claim 89, wherein said authority record includes at least one nonce.

119. The system of Claim 118, further comprising means for encrypting said nonce with a public key.

120. The system of Claim 89, wherein said authority record includes at least one time value associated with processing of a portion of data stored on said storage device.

121. The system of Claim 120, wherein said time value is selected from the group consisting of a start time and an end time.

122. The system of Claim 89, further comprising means for storing call authentication data on said storage device.